

© EPODOC / EPO

PN - JP2000286840 A 20001013
 PD - 2000-10-13
 PR - JP19990094197 19990331
 OPD - 1999-03-31
 TI - ACCESS CONTROL SYSTEM
 IN - ICHISE NORIYOSHI
 PA - NIPPON ELECTRIC CO
 IC - H04L9/32 ; G06F12/14 ; G09C1/00

© WPI / DERWENT

TI - Access control system judges whether disclosure key input by user is in accordance with secret key, based on which corresponding access control information is attained and access control of object is performed

PR - JP19990094197 19990331

PN - JP2000286840 A 20001013 DW200102 H04L9/32 008pp

PA - (NIDE) NEC CORP

IC - G06F12/14 ;G09C1/00 ;H04L9/32

AB - JP2000286840 NOVELTY - A verifying unit (11) judges whether a disclosure key (22) input by an user (21) corresponds to secret key (23). A controller (13), extracts access control information corresponding to disclosure key from a memory (12). The verification unit and controller exchanges information using a window (14). When the disclosure key corresponds to secret key, access control of the object (6) is performed.

- USE - For data access control system.
- ADVANTAGE - Avoids need of performing intensive user management for performing access control.
- DESCRIPTION OF DRAWING(S) - The figure shows the block diagram of the access control system.
- Object 6
- Verifying unit 11
- Memory 12
- Controller 13
- Window 14
- User 21
- Disclosure key 22
- Secret key 23
- (Dwg.1/6)

OPD - 1999-03-31

AN - 2001-011688 [02]

© PAJ / JPO

PN - JP2000286840 A 20001013

PD - 2000-10-13

AP - JP19990094197 19990331

IN - ICHISE NORIYOSHI

PA - NEC CORP

TI - ACCESS CONTROL SYSTEM

AB - PROBLEM TO BE SOLVED: To provide an access control system that can distinguish users and that can conduct access control without the need for intensive user management.

- SOLUTION: The access control system is provided with a user key certification means 11 that discriminates whether or not a public key 22 entered by a user 21 corresponds to a private key 23 of the user, an access control information group 12 that stores access control information corresponding to the public key 22, an object access means 13 that applies access control to an object 6 corresponding to the public key 22 on the basis of the access control information obtained from the access control information group 12, and a window means 14 that enters the public key 22 and that exchanges information with the user key certification means 11 and the object access means 13. The system conducts access control according to the access control information when it is discriminated that the public key 22 corresponds to the private key 23 with respect to the access request of the entered object 6.

I - H04L9/32 ;G06F12/14 ;G09C1/00

PATENT ABSTRACTS OF JAPAN

(11) Publication number : 2000-286840

(43) Date of publication of application : 13.10.2000

(51) Int. Cl.

H04L 9/32

G06F 12/14

G09C 1/00

(21) Application number : 11-094197 (71) Applicant : NEC CORP

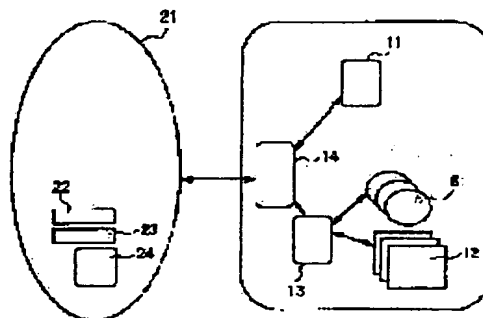
(22) Date of filing : 31.03.1999 (72) Inventor : ICHISE NORIYOSHI

(54) ACCESS CONTROL SYSTEM

(57) Abstract:

PROBLEM TO BE SOLVED: To provide an access control system that can distinguish users and that can conduct access control without the need for intensive user management.

SOLUTION: The access control system is provided with a user key certification means 11 that discriminates whether or not a public key 22 entered by a user 21 corresponds to a private key 23 of the user, an access control information group 12 that stores access control information corresponding to the public key 22, an object access means 13 that applies access control to an object 6 corresponding to the public key 22 on the basis of the access control information obtained from the access control information group 12, and a window means 14 that enters the public key 22 and that exchanges information with the user key certification means 11 and the object access means 13. The system conducts access control according to the access control information when it is discriminated that the public key 22 corresponds to the private key 23 with respect to the access request of the entered object 6.



LEGAL STATUS

[Date of request for examination] 02.03.2000

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's
decision of rejection]

[Date of requesting appeal against
examiner's decision of rejection]

[Date of extinction of right]

Copyright (C); 1998, 2003 Japan Patent Office

* NOTICES *

Japan Patent Office is not responsible for any damages caused by the use of this translation.

1. This document has been translated by computer. So the translation may not reflect the original precisely.
2. **** shows the word which can not be translated.
3. In the drawings, any words are not translated.

DETAILED DESCRIPTION

[Detailed Description of the Invention]

[0001]

[The technical field to which invention belongs] This invention relates to the access-control system which distinguishes a user and performs an access control, without performing user management intensively.

[0002]

[Description of the Prior Art] Drawing 5 is the block diagram showing the conventional access-control system, and this access-control system is constituted by the window equipment 5 and the object 6 which receive the information for authentication from user authentication equipment 1, the user password information group 2, the access-control information group 3, object access equipment 4, and a user. In addition, a user 7 has the user id8 and password 9 which are a user's authentication information.

[0003] Next, actuation of this access-control system is explained based on drawing 6. If window equipment 5 receives a user id8 and a password 9 from a user 7, this window equipment 5 will pass the user id8 and password 9 which were received to user authentication equipment 1 (step A1). Subsequently, with user authentication equipment 1, the password 9 corresponding to a user id8 judges whether it is the right by the user password information group 2, and this judgment result is returned to window equipment 5 (step A2).

[0004] Window equipment 5 will refuse the demand from a user 7, if a password 9 is right and waiting (step A3) and a password 9 have made a mistake in the demand from a user 7. Subsequently, if the demand of existing access to a certain object 6 from a user 7 is made by window equipment 5, window equipment 5 will pass this demand and user id8 to object access equipment 4 (step B1). Object access equipment 4 obtains the propriety of access to the demanded object to the passed user id8 from the access-control information group 3 (step B-2). If this access is possible, access to the demanded object will be performed (step B3).

[0005]

[Problem(s) to be Solved by the Invention] By the way, in the conventional access-control system, in order to distinguish a user and to perform an access control, in order that the user id8 whom a user 7 presents might judge whether it is the right, password information had to be managed by the user password information group 2, and there was a trouble that it was necessary to manage User Information intensively.

[0006] This invention aims at offering the access-control system which can distinguish a user and can perform an access control, without being made in view of the above-mentioned situation, and performing user management intensively.

[0007]

[Means for Solving the Problem] In order to solve the above-mentioned technical problem, this invention offered the following access-control systems. Namely, an access-control system according to claim 1 A user key certification means to judge whether a public key inputted by user corresponds to a secret key which said user has, An access-control information group which memorizes control information of access corresponding to said public key, While inputting said public key as an object access means to perform an access control to an object corresponding to said public key, based on access-control information acquired from this access-control information group It has said user key

certification means and said object access means with each, and a window means to perform an informational exchange. When judged with said public key corresponding to said secret key to an access request to an inputted object, it is characterized by performing an access control according to said access-control information.

[0008] A user key certification means by which a public key into which an access-control system according to claim 2 was inputted by user judges whether it corresponds to a secret key which said user has, An access-control information group which memorizes control information of access corresponding to said public key, While inputting said public key as an object access means to perform an access control to an object corresponding to said public key, based on access-control information acquired from this access-control information group An exchange of said user key certification means, and said object access means with each and information is performed. It has a shell means to perform processing which followed this access request when a compounded access request was made. When judged with said public key corresponding to said secret key to an access request to an inputted object, it is characterized by performing an access control according to said access-control information.

[0009]

[Embodiment of the Invention] Each operation gestalt of the access-control system of this invention is explained based on a drawing.

[Operation gestalt of ** 1st] drawing 1 is the block diagram showing the access-control system of the 1st operation gestalt of this invention, and this access-control system is constituted by user key certification equipment (user key certification means) 11, the access-control information group 12, object access equipment (object access means) 13, window equipment (window means) 14, and the object 6. Moreover, a user 21 has a public key 22, the secret key 23, and signature equipment 24.

[0010] User key certification equipment 11 judges whether this user 21 has the public key 22 of the arbitration by the public key system, and the secret key 23 to the public key 22 which the user 21 presented to the user 21 who has the secret key 23 corresponding to it, and sends out the judgment result. That is, while obtaining a public key 22, the value which signed the delivery this character string with the secret key 23 in the character string is verified with reception, the signature is verified with a public key 22, and it returns whether a public key 22 is just.

[0011] The access-control information group 12 has the use good improper information for every public key 22 to each access classification of each object 6, and has memorized the control information of access corresponding to the public key 22 of the user 21 of this access request origin to each access request to each object 6.

[0012] Object access equipment 13 performs the access control according to the public key 22 corresponding to the user 21 of this access request origin to the access request to an object 6 using the information acquired from the access-control information group 12. That is, to the access request to an object 6, the propriety of the access classification to the demanded object 6 to a public key 22 is obtained, and when the permission is granted by the access-control information group 12, demanded access is performed from it.

[0013] Window equipment 14 performs agency with a user 21, and user key certification equipment 11 and object access equipment 13, and when reception and a public key 22 are just, it memorizes this public key 22 for the access request and public key 22 from a user to an object.

[0014] Next, actuation of this access-control system is explained based on drawing 2. First, if window equipment 14 receives a public key 22 from a user 21, this public key 22 will be passed to user key certification equipment 11 (step C1). Subsequently, the character string of arbitration is returned to window equipment 14, and, as for delivery and window equipment 14, user key certification equipment 11 returns this character string to a user 21 (step C2). Through signature equipment 24, window equipment 14 obtains the data which signed this character string with the secret key 23, and a user 21 hands it to user key certification equipment 11 (step C3).

[0015] User key certification equipment 11 tells that a public key 22 is just to window equipment 14, when the passed data is verified with a public key 22 (step C4) and it is able to be checked that a public key 22 is just. Window equipment 14 memorizes this public key 22, when a public key 22 is just (step C5).

[0016] Subsequently, if the demand of existing access to the object 6 which is in window equipment

14 from a user 21 occurs, this window equipment 14 will pass this access request and public key 22 to object access equipment 13 (step D1). Object access equipment 13 obtains the propriety of this access to this demanded object 6 to this user's 21 public key 22 from the access-control information group 12 (step D2). Here, if this access is possible, access to this object 6 will be performed (step D3).

[0017] Here, actuation of this access-control system is explained to details using an example. first -- a window -- equipment -- 14 -- a user -- 21 -- from -- having obtained -- 128 -- bit -- a public key -- 22 -- " -- asdfjkl;asdfjkl --; -- " -- a user -- a key -- certification -- equipment -- 11 -- delivery -- a user -- a key -- certification -- equipment -- 11 -- returning -- arbitration -- a character string -- " -- 0123456789 -- ABCDEF -- " -- a user 21 -- returning .

[0018] If there is no mistake in the value which user key certification equipment 11 obtained value";lkjfdsa;lkjfdsa" which signed the character string handed by the user 21 with the secret key 23 corresponding to a public key 22 from window equipment 14, verified it with the public key 22, and signed this character string with the secret key 23 corresponding to a public key 22, that will be told to window equipment 14 and window equipment 14 will memorize a public key 22.

[0019] Subsequently, when the read request from a user 21 to file "c:\autoexec.bat" of an object 6 occurs, window equipment 14 passes this read request and public key 22 to object access equipment 13. Object access equipment 13 investigates whether reading by file "c:\autoexec.bat" is permitted to the public key 22, and if the permission is granted by the access-control information group 12, it will perform reading by this file from it.

[0020] The access control for every user 21 to an object 6 can be performed without managing User Information, since according to this operation gestalt the public key 22 which a user 21 has with a public key system is checked and this public key 22 performs the access control to an object 6.

[0021] [Operation gestalt of ** 2nd] drawing 3 is the block diagram showing the access-control system of the 2nd operation gestalt of this invention, and this access-control system is constituted by user key certification equipment (user key certification means) 31, the access-control information group 12, object access equipment 13, shell equipment (shell means) 32, demand encryption equipment 33, and the object 6. Moreover, a user 21 has a public key 22 and the secret key 23.

[0022] User key certification equipment 31 will return the demand message which **** data, if the data and the public key 22 which enciphered the demand message with the secret key 23 are compounded with reception, data is compounded with a public key 22 and **** is successful. The access-control information group 12 has the use good improper information for every public key 22 to each access classification of each object 6. To the access request to an object 6, object access equipment 13 obtains the propriety of the access classification to the demanded object 6 to a public key 22, and when the permission is granted by the access-control information group 12, it performs demanded access from it.

[0023] Shell equipment 32 passes an access request and a public key 22 to object access equipment 13, when processing which followed the demand when delivery and the compounded demand message were obtained by user key certification equipment 31 in the data and the public key 22 which were received from demand encryption equipment 33, and which were enciphered is performed and the access request to an object 6 occurs in it. Demand encryption equipment 33 passes what enciphered the demand message from a user 21 with a user's 21 secret key 23 to shell equipment 32 with a public key 22.

[0024] Next, actuation of this access-control system is explained based on drawing 4. First, shell equipment 32 receives what enciphered the demand message from a user 21 with a user's 21 secret key 23 with a public key 22 with demand encryption equipment 33 (step E1). Subsequently, shell equipment 32 passes the data and the public key 22 which were received from demand encryption equipment 33 and which were enciphered to user key certification equipment 31 (step E2).

[0025] User key certification equipment 31 compounds with reception the data and the public key 22 which enciphered the demand message with the secret key 23, data is compounded with a public key 22 (step E3), and if **** is successful, the demand message which **** data will be returned to shell equipment 32 (step E4). Shell equipment 32 performs processing according to a demand, when the compounded demand message is obtained (step E5).

[0026] When there is an access request to an object 6 in this processing, shell equipment 32 passes

an access request and a public key 22 to object access equipment 13 (step F1). To the access request to an object 6, object access equipment 13 obtains the propriety of the access classification to the demanded object 6 to a public key 22, and when the permission is granted by the access-control information group 12, it performs demanded access from it (step F2).

[0027] Here, actuation of this access-control system is explained to details using an example. First, the data which enciphered the script containing the read request of file "c:\autoexec.bat" of the object 6 from a user 21 with a user's 21 secret key 23 is passed to shell equipment 32 with a public key 22 from demand encryption equipment 33 (step E1).

[0028] Subsequently, shell equipment 32 passes the data and the public key 22 which were received from demand encryption equipment 33 and which were enciphered to user key certification equipment 31 (step E2). If user key certification equipment 31 compounds with reception the data and the public key 22 which enciphered the demand message with the secret key 23, this data is compounded with a public key 22 (step E3) and **** is successful, the script which **** data will be returned to shell equipment 32 (step E4).

[0029] Shell equipment 32 performs this script, when the compounded script is obtained (step E5). When there is a read request of file "c:\autoexec.bat" in this script, shell equipment 32 passes this access request and a public key 22 to object access equipment 13 (step F1).

[0030] To the read request to this file "c:\autoexec.bat", object access equipment 13 obtains the propriety [file / to a public key 22 / that was demanded / this] of reading from the access-control information group 12, and when the permission is granted, it reads (step F2).

[0031] The access control for every user 21 to an object 6 can be performed without managing User Information, since according to this operation gestalt the public key 22 which a user 21 has with a public key system is checked like the 1st operation gestalt mentioned above and this public key 22 performs the access control to an object 6. As mentioned above, although each operation gestalt of the access-control system of this invention has been explained based on a drawing, modification of layout etc. is possible for a concrete configuration in the range which is not limited to each operation gestalt and does not deviate from the summary of this invention.

[0032]

[Effect of the Invention] The access control for every user can be performed without managing User Information like, according to the access-control system of this invention, since the public key which was explained above and which a user has with a public key system is checked and this public key performs an access control. Therefore, without performing user management intensively, a user can be distinguished and an access control can be performed.

[Translation done.]

(11)特許出願公開番号

特開2000-286840

(P2000-286840A)

(43)公開日 平成12年10月13日(2000. 10. 13)

(51)Int.Cl. ⁷	識別記号	F I	テマコード ⁸ (参考)
H 0 4 L 9/32		H 0 4 L 9/00	6 7 5 B 5 B 0 1 7
G 0 6 F 12/14	3 2 0	G 0 6 F 12/14	3 2 0 B 5 J 1 0 4
G 0 9 C 1/00	6 4 0	G 0 9 C 1/00	6 4 0 B 9 A 0 0 1

審査請求 有 請求項の数2 O.L (全 8 頁)

(21)出願番号 特願平11-94197

(22)出願日 平成11年3月31日(1999. 3. 31)

(71)出願人 000004237
日本電気株式会社
東京都港区芝五丁目7番1号

(72)発明者 市瀬 規善
東京都港区芝五丁目7番1号 日本電気株
式会社内

(74)代理人 100108578
弁理士 高橋 韶男 (外3名)

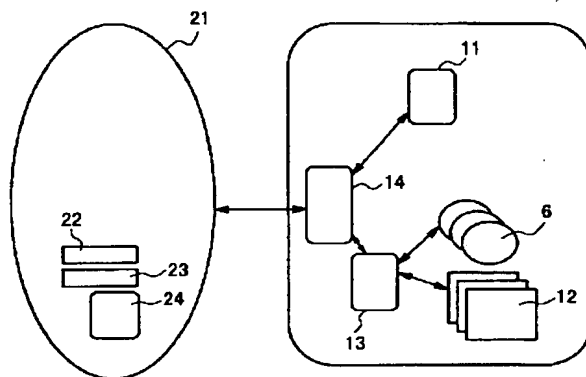
Fターム(参考) 5B017 AA01 BA07 BB02 CA16
5J104 AA07 AA09 KA01 KA05 KA06
LA03 LA06 NA02 NA05 PA07
9A001 EE03 FZ06 LL03

(54) 【発明の名称】 アクセス制御システム

(57) 【要約】

【課題】 ユーザ管理を集中的に行うことなしに、ユーザを区別しアクセス制御を行うことができるアクセス制御システムを提供する。

【解決手段】 ユーザ２１により入力された公開鍵２２がユーザの有する非公開鍵２３に対応するか否かを判定するユーザ鍵証明手段１１と、公開鍵２２に対応するアクセスの制御情報を記憶するアクセス制御情報群１２と、アクセス制御情報群１２から得られるアクセス制御情報に基づき公開鍵２２に対応するオブジェクト６へのアクセス制御を行うオブジェクトアクセス手段１３と、公開鍵２２を入力するとともにユーザ鍵証明手段１１及びオブジェクトアクセス手段１３各々と情報のやり取りを行う窓口手段１４とを備え、入力されたオブジェクト６へのアクセス要求に対し、公開鍵２２が非公開鍵２３に対応すると判定された場合にアクセス制御情報にしたがってアクセス制御を行うことを特徴とする。



【特許請求の範囲】

【請求項1】 ユーザにより入力された公開鍵が前記ユーザの有する非公開鍵に対応するか否かを判定するユーザ鍵証明手段と、

前記公開鍵に対応するアクセスの制御情報を記憶するアクセス制御情報群と、

該アクセス制御情報群から得られるアクセス制御情報に基づき、前記公開鍵に対応するオブジェクトへのアクセス制御を行うオブジェクトアクセス手段と、

前記公開鍵を入力するとともに、前記ユーザ鍵証明手段及び前記オブジェクトアクセス手段各々と情報のやり取りを行う窓口手段とを備え、

入力されたオブジェクトへのアクセス要求に対し、前記公開鍵が前記非公開鍵に対応すると判定された場合に、前記アクセス制御情報にしたがってアクセス制御を行うことを特徴とするアクセス制御システム。

【請求項2】 ユーザにより入力された公開鍵が前記ユーザの有する非公開鍵に対応するか否かを判定するユーザ鍵証明手段と、

前記公開鍵に対応するアクセスの制御情報を記憶するアクセス制御情報群と、

該アクセス制御情報群から得られるアクセス制御情報に基づき、前記公開鍵に対応するオブジェクトへのアクセス制御を行うオブジェクトアクセス手段と、

前記公開鍵を入力するとともに、前記ユーザ鍵証明手段及び前記オブジェクトアクセス手段各々と情報のやり取りを行ない、複合されたアクセス要求がなされた場合に、該アクセス要求にしたがった処理を行うシェル手段とを備え、

入力されたオブジェクトへのアクセス要求に対し、前記公開鍵が前記非公開鍵に対応すると判定された場合に、前記アクセス制御情報にしたがってアクセス制御を行うことを特徴とするアクセス制御システム。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、ユーザ管理を集中的に行うことなく、ユーザを区別しアクセス制御を行うアクセス制御システムに関するものである。

【0002】

【従来の技術】図5は従来のアクセス制御システムを示す構成図であり、このアクセス制御システムは、ユーザ認証装置1、ユーザパスワード情報群2、アクセス制御情報群3、オブジェクトアクセス装置4、ユーザから認証のための情報を受け取る窓口装置5及びオブジェクト6により構成されている。なお、ユーザ7は、ユーザの認証情報であるユーザid8とパスワード9を有する。

【0003】次に、このアクセス制御システムの動作について図6に基づき説明する。窓口装置5がユーザ7からユーザid8とパスワード9を受け取ると、この窓口装置5は受け取ったユーザid8とパスワード9をユー

ザ認証装置1に渡す(ステップA1)。次いで、ユーザ認証装置1では、ユーザパスワード情報群2によりユーザid8に対応するパスワード9が正しいか否かを判定し、この判定結果を窓口装置5に返す(ステップA2)。

【0004】窓口装置5は、パスワード9が正しければユーザ7からの要求を待ち(ステップA3)、パスワード9が間違っていればユーザ7からの要求を拒否する。次いで、窓口装置5に、ユーザ7からあるオブジェクト6へのあるアクセスの要求がなされると、窓口装置5は、オブジェクトアクセス装置4へこの要求とユーザid8を渡す(ステップB1)。オブジェクトアクセス装置4は、渡されたユーザid8に対する要求されたオブジェクトへのアクセスの可否をアクセス制御情報群3より得る(ステップB2)。このアクセスが可能であれば、要求されたオブジェクトへのアクセスを行う(ステップB3)。

【0005】

【発明が解決しようとする課題】ところで、従来のアクセス制御システムにおいては、ユーザを区別しアクセス制御を行うには、ユーザ7の呈示するユーザid8が正しいか否かを判定するために、ユーザパスワード情報群2によりパスワード情報を管理しなければならず、ユーザ情報を集中的に管理する必要があるという問題点があった。

【0006】本発明は、上記の事情に鑑みてなされたものであって、ユーザ管理を集中的に行うことなしに、ユーザを区別しアクセス制御を行うことができるアクセス制御システムを提供することを目的とする。

【0007】

【課題を解決するための手段】上記課題を解決するために、本発明は次の様なアクセス制御システムを提供した。すなわち、請求項1記載のアクセス制御システムは、ユーザにより入力された公開鍵が前記ユーザの有する非公開鍵に対応するか否かを判定するユーザ鍵証明手段と、前記公開鍵に対応するアクセスの制御情報を記憶するアクセス制御情報群と、該アクセス制御情報群から得られるアクセス制御情報に基づき、前記公開鍵に対応するオブジェクトへのアクセス制御を行うオブジェクトアクセス手段と、前記公開鍵を入力するとともに、前記ユーザ鍵証明手段及び前記オブジェクトアクセス手段各々と情報のやり取りを行う窓口手段とを備え、入力されたオブジェクトへのアクセス要求に対し、前記公開鍵が前記非公開鍵に対応すると判定された場合に、前記アクセス制御情報にしたがってアクセス制御を行うことを特徴としている。

【0008】請求項2記載のアクセス制御システムは、ユーザにより入力された公開鍵が前記ユーザの有する非公開鍵に対応するか否かを判定するユーザ鍵証明手段と、前記公開鍵に対応するアクセスの制御情報を記憶す

るアクセス制御情報群と、該アクセス制御情報群から得られるアクセス制御情報に基づき、前記公開鍵に対応するオブジェクトへのアクセス制御を行うオブジェクトアクセス手段と、前記公開鍵を入力するとともに、前記ユーザ鍵証明手段及び前記オブジェクトアクセス手段各々と情報のやり取りを行ない、複合されたアクセス要求がなされた場合に該アクセス要求にしたがった処理を行うシェル手段とを備え、入力されたオブジェクトへのアクセス要求に対し、前記公開鍵が前記非公開鍵に対応すると判定された場合に、前記アクセス制御情報にしたがってアクセス制御を行うことを特徴としている。

【0009】

【発明の実施の形態】本発明のアクセス制御システムの各実施形態について図面にに基づき説明する。

〔第1の実施形態〕図1は本発明の第1の実施形態のアクセス制御システムを示す構成図であり、このアクセス制御システムは、ユーザ鍵証明装置（ユーザ鍵証明手段）11、アクセス制御情報群12、オブジェクトアクセス装置（オブジェクトアクセス手段）13、窓口装置（窓口手段）14及びオブジェクト6により構成されている。また、ユーザ21は、公開鍵22、非公開鍵23及び署名装置24を有する。

【0010】ユーザ鍵証明装置11は、公開鍵方式による任意の公開鍵22とそれに対応する非公開鍵23を有するユーザ21に対し、ユーザ21が呈示した公開鍵22に対する非公開鍵23を該ユーザ21が有するか否かを判定し、その判定結果を送出する。すなわち、公開鍵22を得るとともに、文字列を渡し該文字列を非公開鍵23で署名した値を受け取り、その署名を公開鍵22によってベリファイし、公開鍵22が正当か否かを返す。

【0011】アクセス制御情報群12は、各オブジェクト6の各アクセス種別に対する公開鍵22毎の利用不可情報を有するもので、各オブジェクト6への各アクセス要求に対する該アクセス要求元のユーザ21の公開鍵22に対応したアクセスの制御情報を記憶している。

【0012】オブジェクトアクセス装置13は、オブジェクト6に対するアクセス要求に対し、アクセス制御情報群12から得られる情報により、このアクセス要求元のユーザ21に対応する公開鍵22に応じたアクセス制御を行う。すなわち、オブジェクト6へのアクセス要求に対し、アクセス制御情報群12より、公開鍵22に対する要求されたオブジェクト6へのアクセス種別の可否を得、許可されている場合は要求されたアクセスを行う。

【0013】窓口装置14は、ユーザ21と、ユーザ鍵証明装置11、オブジェクトアクセス装置13との仲介を行うもので、ユーザからオブジェクトへのアクセス要求及び公開鍵22を受け取り、公開鍵22が正当である場合に、この公開鍵22を記憶する。

【0014】次に、このアクセス制御システムの動作に

ついて、図2に基づき説明する。まず、窓口装置14がユーザ21から公開鍵22を受け取ると、この公開鍵22をユーザ鍵証明装置11に渡す（ステップC1）。次いで、ユーザ鍵証明装置11が任意の文字列を窓口装置14に渡し、窓口装置14は該文字列をユーザ21に返す（ステップC2）。窓口装置14は、署名装置24を介してユーザ21が該文字列を非公開鍵23で署名したデータを得、ユーザ鍵証明装置11に渡す（ステップC3）。

【0015】ユーザ鍵証明装置11は、渡されたデータを公開鍵22でベリファイし（ステップC4）、公開鍵22が正当であることが確認できた場合、窓口装置14に公開鍵22が正当であることを伝える。窓口装置14は、公開鍵22が正当である場合に、この公開鍵22を記憶する（ステップC5）。

【0016】次いで、窓口装置14にユーザ21からのあるオブジェクト6へのあるアクセスの要求が発生すると、この窓口装置14は、オブジェクトアクセス装置13へこのアクセス要求および公開鍵22を渡す（ステップD1）。オブジェクトアクセス装置13は、アクセス制御情報群12より該ユーザ21の公開鍵22に対する要求された該オブジェクト6への該アクセスの可否を得る（ステップD2）。ここで、このアクセスが可能であれば、このオブジェクト6へのアクセスを行う（ステップD3）。

【0017】ここで、このアクセス制御システムの動作について、具体例を用いて詳細に説明する。まず、窓口装置14がユーザ21から得た128bitの公開鍵22"as d f j k l ; a s d f j k l ;"をユーザ鍵証明装置11に渡し、ユーザ鍵証明装置11が返す任意の文字列"0 1 2 3 4 5 6 7 8 9 A B C D E F"をユーザ21に返す。

【0018】ユーザ鍵証明装置11は、ユーザ21から渡される文字列を公開鍵22に対応する非公開鍵23で署名した値"l k j f d s a ; l k j f d s a"を窓口装置14から得、公開鍵22でベリファイし、該文字列を公開鍵22に対応する非公開鍵23で署名した値に間違いが無ければ、その旨を窓口装置14に伝え、窓口装置14は公開鍵22を記憶する。

【0019】次いで、ユーザ21からオブジェクト6のファイル"c : ¥ a u t o e x e c . b a t"への読み取り要求が発生した場合、窓口装置14は、この読み取り要求および公開鍵22をオブジェクトアクセス装置13に渡す。オブジェクトアクセス装置13は、アクセス制御情報群12より、公開鍵22に対しファイル"c : ¥ a u t o e x e c . b a t"への読み取りが許可されているか否かを調べ、許可されていれば、このファイルへの読み取りを行う。

【0020】本実施形態によれば、公開鍵方式によりユーザ21の有する公開鍵22を確認し、かつ該公開鍵2

2によりオブジェクト6へのアクセス制御を行うので、ユーザ情報を管理することなく、オブジェクト6へのユーザ21毎のアクセス制御を行うことができる。

【0021】〔第2の実施形態〕図3は本発明の第2の実施形態のアクセス制御システムを示す構成図であり、このアクセス制御システムは、ユーザ鍵証明装置（ユーザ鍵証明手段）31、アクセス制御情報群12、オブジェクトアクセス装置13、シェル装置（シェル手段）32、要求暗号化装置33及びオブジェクト6により構成されている。また、ユーザ21は、公開鍵22及び非公開鍵23を有する。

【0022】ユーザ鍵証明装置31は、要求メッセージを非公開鍵23で暗号化したデータと公開鍵22とを受け取り、データを公開鍵22によって複合し、復合が成功したら、データを復合したものである要求メッセージを返す。アクセス制御情報群12は、各オブジェクト6の各アクセス種別に対する公開鍵22毎の利用可不可情報を有する。オブジェクトアクセス装置13は、オブジェクト6へのアクセス要求に対し、アクセス制御情報群12より、公開鍵22に対する要求されたオブジェクト6へのアクセス種別の可否を得、許可されている場合は要求されたアクセスを行う。

【0023】シェル装置32は、要求暗号化装置33より受け取った暗号化されたデータおよび公開鍵22をユーザ鍵証明装置31に渡し、複合された要求メッセージが得られた場合に、要求にしたがった処理を実行し、その中でオブジェクト6へのアクセス要求が発生した場合に、オブジェクトアクセス装置13に、アクセス要求および公開鍵22を渡す。要求暗号化装置33は、ユーザ21からの要求メッセージをユーザ21の非公開鍵23により暗号化したものを、公開鍵22と共にシェル装置32に渡す。

【0024】次に、このアクセス制御システムの動作について、図4に基づき説明する。まず、要求暗号化装置33によりユーザ21からの要求メッセージをユーザ21の非公開鍵23により暗号化したものを、シェル装置32が公開鍵22と共に受け取る（ステップE1）。次いで、シェル装置32は、要求暗号化装置33より受け取った暗号化されたデータおよび公開鍵22を、ユーザ鍵証明装置31に渡す（ステップE2）。

【0025】ユーザ鍵証明装置31は、要求メッセージを非公開鍵23で暗号化したデータと公開鍵22とを受け取り、データを公開鍵22によって複合し（ステップE3）、復合が成功したらデータを復合したものである要求メッセージをシェル装置32に返す（ステップE4）。シェル装置32は、複合された要求メッセージがえられた場合に、要求にしたがった処理を実行する（ステップE5）。

【0026】この処理の中で、オブジェクト6へのアクセス要求があった場合に、シェル装置32は、オブジェ

クトアクセス装置13にアクセス要求および公開鍵22を渡す（ステップF1）。オブジェクトアクセス装置13は、オブジェクト6へのアクセス要求に対し、アクセス制御情報群12より、公開鍵22に対する要求されたオブジェクト6へのアクセス種別の可否を得、許可されている場合には要求されたアクセスを行う（ステップF2）。

【0027】ここで、このアクセス制御システムの動作について、具体例を用いて詳細に説明する。まず、要求暗号化装置33より、ユーザ21からのオブジェクト6のファイル“c:\autoexec.bat”の読み取り要求を含むスクリプトをユーザ21の非公開鍵23により暗号化したデータを、公開鍵22とともにシェル装置32に渡す（ステップE1）。

【0028】次いで、シェル装置32は、要求暗号化装置33より受け取った暗号化されたデータおよび公開鍵22を、ユーザ鍵証明装置31に渡す（ステップE2）。ユーザ鍵証明装置31は、要求メッセージを非公開鍵23で暗号化したデータと公開鍵22とを受け取り、このデータを公開鍵22によって複合し（ステップE3）、復合が成功したら、データを復合したものであるスクリプトをシェル装置32に返す（ステップE4）。

【0029】シェル装置32は、複合されたスクリプトが得られた場合に、このスクリプトを実行する（ステップE5）。このスクリプトの中で、ファイル“c:\autoexec.bat”の読み取り要求があった場合に、シェル装置32は、オブジェクトアクセス装置13に、該アクセス要求および公開鍵22を渡す（ステップF1）。

【0030】オブジェクトアクセス装置13は、このファイル“c:\autoexec.bat”への読み取り要求に対し、アクセス制御情報群12より公開鍵22に対する要求された該ファイルへの読み取りの可否を得、許可されている場合には読み取りを行う（ステップF2）。

【0031】本実施形態によれば、上述した第1の実施形態と同様に、公開鍵方式によりユーザ21の有する公開鍵22を確認し、かつ該公開鍵22によりオブジェクト6へのアクセス制御を行うので、ユーザ情報を管理することなく、オブジェクト6へのユーザ21毎のアクセス制御を行うことができる。以上、本発明のアクセス制御システムの各実施形態について図面に基づき説明してきたが、具体的な構成は各実施形態に限定されるものではなく、本発明の要旨を逸脱しない範囲で設計の変更等が可能である。

【0032】

【発明の効果】以上説明した様に、本発明のアクセス制御システムによれば、公開鍵方式によりユーザの有する公開鍵を確認し、かつ該公開鍵によりアクセス制御を行

うので、ユーザ情報を管理することなく、ユーザ毎のアクセス制御を行うことができる。したがって、ユーザ管理を集中的に行うことなしに、ユーザを区別しアクセス制御を行うことができる。

【図面の簡単な説明】

【図1】 本発明の第1の実施形態のアクセス制御システムを示す構成図である。

【図2】 本発明の第1の実施形態のアクセス制御システムの動作を示す流れ図である。

【図3】 本発明の第2の実施形態のアクセス制御システムを示す構成図である。

【図4】 本発明の第2の実施形態のアクセス制御システムの動作を示す流れ図である。

【図5】 従来のアクセス制御システムを示す構成図である。

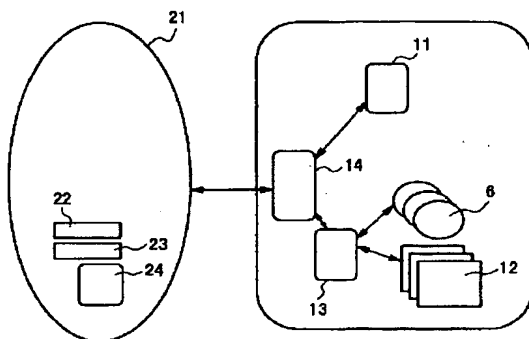
【図6】 従来のアクセス制御システムの動作を示す流れ図である。

【符号の説明】

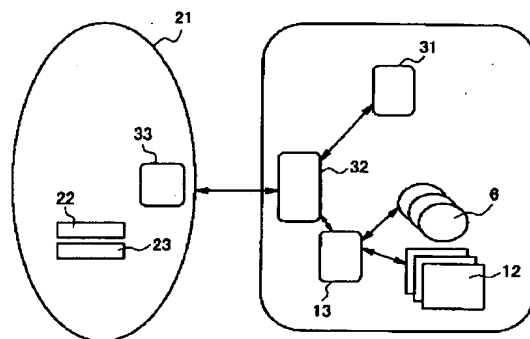
- 1 ユーザ認証装置
- 2 ユーザパスワード情報群

- 3 アクセス制御情報群
- 4 オブジェクトアクセス装置
- 5 窓口装置
- 6 オブジェクト
- 7 ユーザ
- 8 ユーザid
- 9 パスワード
- 11 ユーザ鍵証明装置（ユーザ鍵証明手段）
- 12 アクセス制御情報群
- 13 オブジェクトアクセス装置（オブジェクトアクセス手段）
- 14 窓口装置（窓口手段）
- 21 ユーザ
- 22 公開鍵
- 23 非公開鍵
- 24 署名装置
- 31 ユーザ鍵証明装置（ユーザ鍵証明手段）
- 32 シェル装置（シェル手段）
- 33 要求暗号化装置

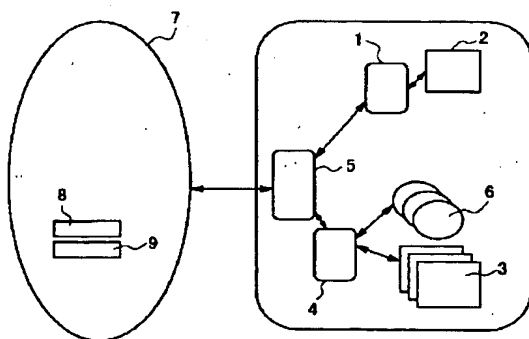
【図1】



【図3】

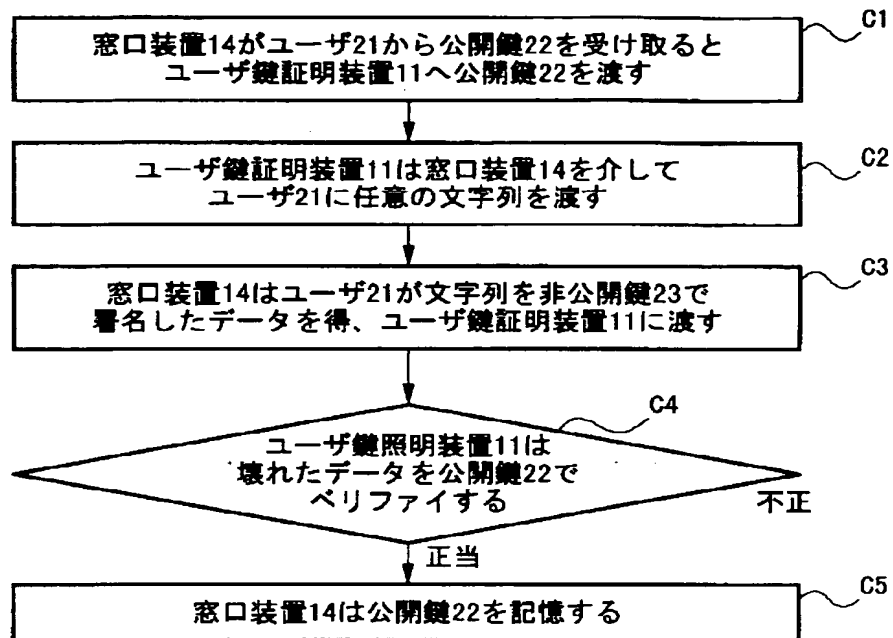


【図5】

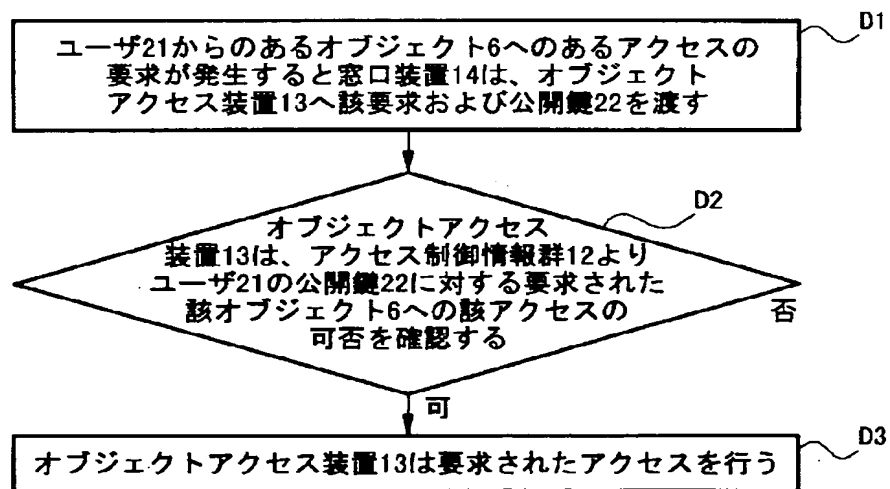


【図2】

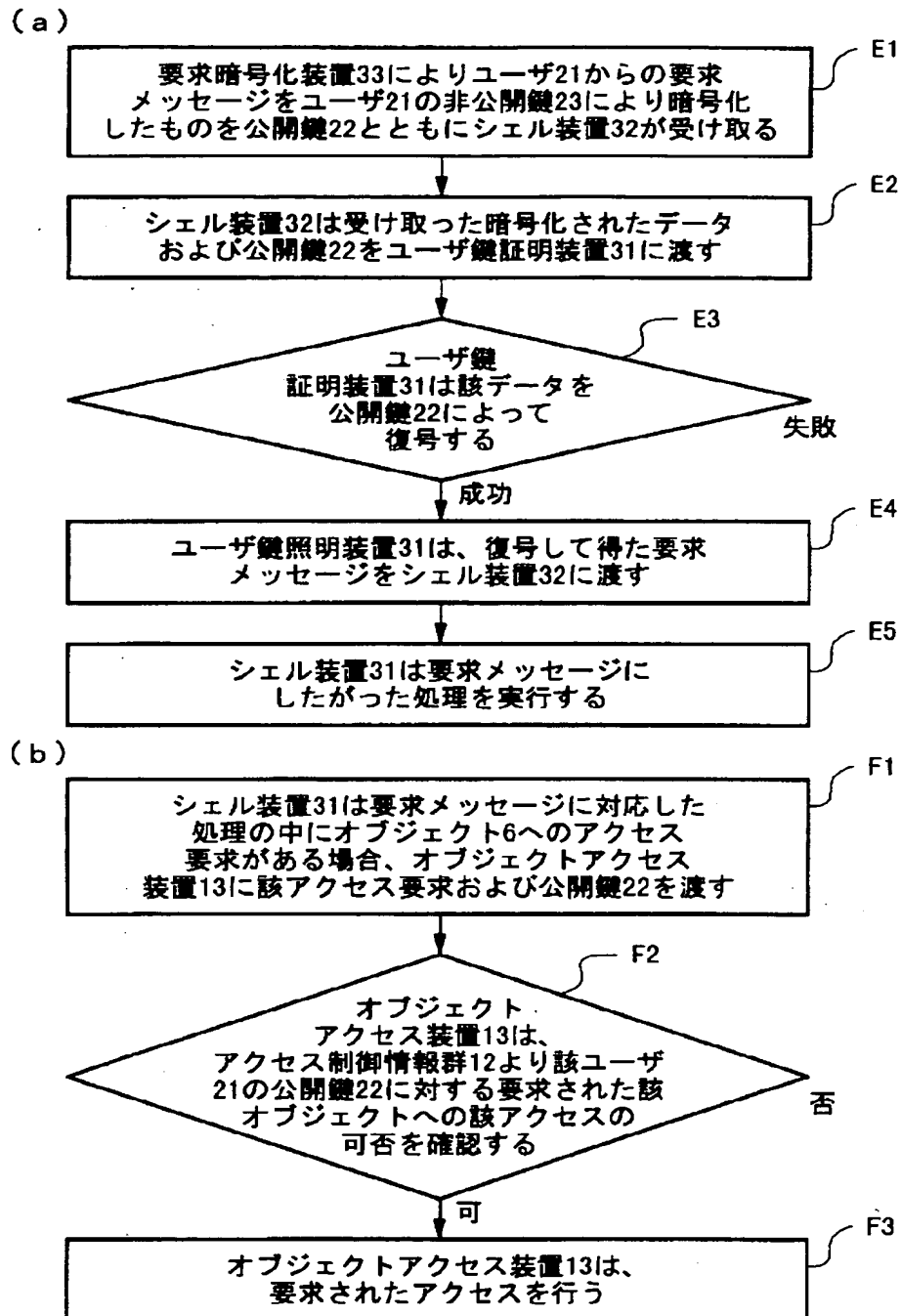
(a)



(b)

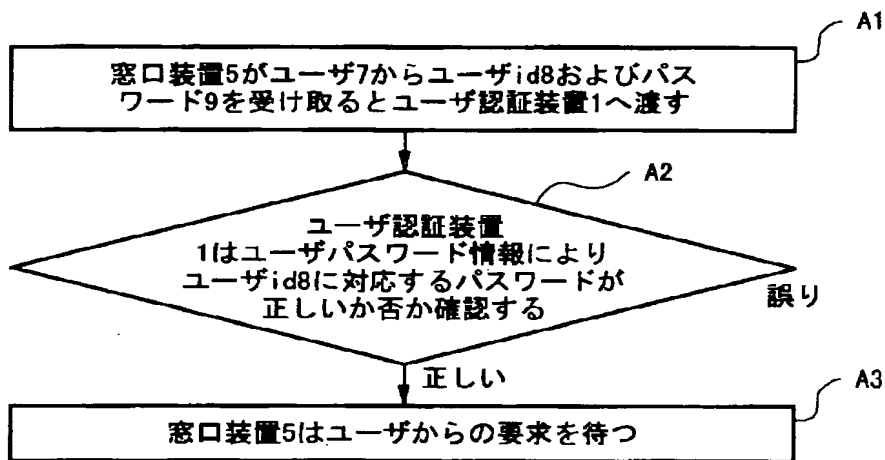


【図4】



【図6】

(a)



(b)

